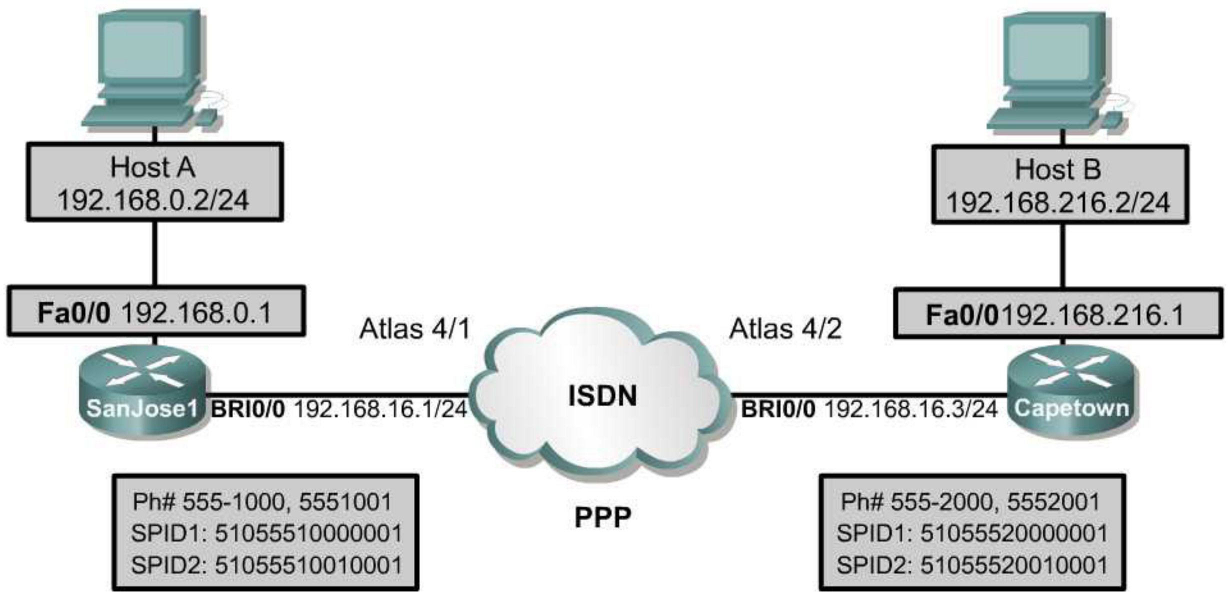
Lab 4.9.1 Configuring ISDN BRI



Objective

In this lab, the student will configure two Cisco routers for DDR using ISDN BRI. The student will also configure PPP CHAP authentication.

Scenario

The International Travel Agency (ITA) wants an ISDN DDR connection configured between a remote office in Capetown and its corporate office known as SanJose1. For security reasons, and to keep ISDN charges to a minimum, suggest that only Web, e-mail, FTP, Telnet, and DNS traffic activate the link from the remote site. Also recommend configuring PPP CHAP authentication. Finally, Capetown connects to a stub network. For this reason, suggest that static and default routes be used between both sites.

Step 1

Before beginning this lab, it is recommended that the routers be reloaded after erasing their startup configuration. This will prevent problems that may be caused by residual configurations.

Build and configure the network according to the diagram, but do not configure the BRI interfaces for either router yet. Use the Adtran Atlas 550 or similar device to simulate the ISDN cloud. If the Atlas 550 is used, be sure to use straight-through cables. Connect both routers to the respective BRI module ports of the Atlas 550 as labeled in the diagram.

Configure the hostname and FastEthernet 0/0 interfaces on each router.

Configure both workstations with their respective IP addresses and default gateways. For example, the router Fa0/0 IP address. Have each host **`ping`** their default gateway to verify connectivity.

Step 2

In global configuration mode on SanJose1, use the following to configure the username and password information for the remote router and an enable password for SanJose1:

```
SanJose1(config)#username Capetown password cisco
SanJose1(config)#enable password cisco
SanJose1(config)#line vty 0 4
SanJose1(config-line)#password cisco
SanJose1(config-line)#login
SanJose1(config-line)#exit
```

Note: Use the enable secret password here, but for the purposes of this lab, an enable password is all that is needed. Later in the lab a telnet to SanJose1 will be preformed, therefore, the virtual terminal configuration is necessary.

Configure SanJose1 to use the appropriate ISDN switch type. The ISP will provide this information and in this case, the International Travel Agency has been told their provider is using the National switch type. Enter the following command:

```
SanJose1(config)#isdn switch-type basic-ni
```

Next, set up a dialer list to use with DDR. This dialer list will be used to identify interesting traffic, that is, traffic for which the ISDN link should be established. The International Travel Agency wants to restrict what constitutes “interesting” traffic. However, at this time use the following command:

```
SanJose1(config)#dialer-list 1 protocol ip permit
```

This permissive command will establish the link for any IP traffic that needs to be routed out the BRI interface. In Step 7, this dialer list will be reconfigured to fulfill the client's requirements completely.

Finally, configure a static route to the Capetown stub network (192.168.216.0/24) as follows:

```
SanJose1(config)#ip route 192.168.216.0 255.255.255.0 192.168.16.3
```

Step 3

Configure the SanJose1 BRI interface with IP address, encapsulation, and authentication settings as follows:

```
SanJose1(config)#interface bri0/0
SanJose1(config-if)#ip address 192.168.16.1 255.255.255.0
SanJose1(config-if)#encapsulation ppp
SanJose1(config-if)#ppp authentication chap
```

In order for this BRI to establish a connection with the service provider’s ISDN switch, configure at least one service profile identifier (SPID). With two B channels, configure two SPIDs. Enter the following commands on SanJose1:

```
SanJose1(config-if)#isdn spid1 51055510000001 5551000
SanJose1(config-if)#isdn spid2 51055510010001 5551001
```

Organizations are typically charged by the minute when making a DDR call. Therefore, it is very important to consider changing the dialer idle-timeout default value of 120 seconds to a lower value. If the connection is idle, the router will wait for this configurable period of time before closing the connection. The International Travel Agency would like an aggressive idle timeout set in order to reduce costs. Use the following command to change the timer:


```
SanJose1(config-if)#dialer idle-timeout 60
```

Next, configure the DDR setting on the BRI interface. Use the **dialer-group 1** command as follows, to associate this interface with the already configured **dialer-list 1**:

```
SanJose1(config-if)#dialer-group 1
```

The **dialer map** command is used by DDR whenever the interface encounters interesting traffic. Now, configure the **dialer map** for this interface:

```
SanJose1(config-if)#dialer map ip 192.168.16.3 name Capetown 5552000
```

Notice that this dialer map command is similar to the dialer maps that were created in previous labs. However, since a modem is not used, no modem-script is required.

Finally, activate the BRI 0/0 interface with the **no shutdown** command. Once the BRI interface is activated, the router will send the SPIDs to the ISDN switch. Informational messages should appear on the screen stating the status of the BRI 0/0 is up, but its B channels, BRI 0/0:1, BRI 0/0:2, are down. The following messages stating that the TEIs are up should be received:

```
01:26:09: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to down
01:26:09: %LINK-3-UPDOWN: Interface BRI0/0:2, changed state to down
01:26:09: %LINK-3-UPDOWN: Interface BRI0/0, changed state to up
01:26:09: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0/0, TEI 64 changed to up
01:26:09: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0/0, TEI 65 changed to up
```

If the preceding messages do not appear, or error messages appear, troubleshoot as necessary.

Next, use the **show isdn status** command to get more specific information regarding the established connection with the ISDN switch. The following shows a sample output:

```
SanJose1#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
    dsl 0, interface ISDN Switchtype = basic-ni
     Layer 1 Status:
    ACTIVE
     Layer 2 Status:
    TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    TEI = 65, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
     Spid Status:
    TEI 64, ces = 1, state = 8(established)
        spid1 configured, spid1 sent, spid1 valid
        Endpoint ID Info: epsf = 0, usid = 70, tid = 1
    TEI 65, ces = 2, state = 8(established)
        spid2 configured, spid2 sent, spid2 valid
        Endpoint ID Info: epsf = 0, usid = 70, tid = 2
     Layer 3 Status:
    0 Active Layer 3 Call(s)
     Activated dsl 0 CCBs = 0
     The Free Channel Mask:  0x80000003
     Total Allocated ISDN CCBs = 0
```

If the SPID status is not established or, if the SPID configuration on the router is changed, issue the **clear interface** command to force the router to resend the SPID to the switch. Executing this command once should be sufficient. However, when using the Atlas 550 with the Cisco IOS, it may be necessary to repeat the command a second or third time.

```
SanJose1#clear interface bri0/0
```


The **debug isdn q921** command may also be used to troubleshoot Layer 2 issues between the router and the ISDN switch.

Once connectivity to the ISDN switch has been verified, issue the **show interface bri0/0** command, as follows:

```
SanJose1#show interface bri0/0
BRI0/0 is up, line protocol is up (spoofing)
Hardware is PQUICC BRI with U interface
Internet address is 10.1.1.1/24
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
<output omitted>
```

The highlighted portion of the output shows that the BRI0/0 interface is up and the line protocol is up or spoofing.

1. Since no ISDN call has been made yet, why did the BRI show “up and up” (spoofing)?

____

____

Now issue the **show ip interface brief** command, as follows:

```
SanJose1#show ip interface brief
Interface         IP-Address     OK?    Method        Status        Protocol
FastEthernet0/0   192.168.0.1    YES    manual        up            up
Serial0/0         unassigned     YES    unset         down          down
BRI0/0            192.168.16.1   YES    manual        up            up
BRI0/0:1          unassigned     YES    unset         down          down
BRI0/0:2          unassigned     YES    unset         down          down
Serial0/1         unassigned     YES    unset         down          down
```

2. What do BRI0/0:1 and BRI0/0:2 refer to?

____

____

3. Why is BRI0/0 up, and BRI0/0:1 down?

____

____

Issue the **show dialer** command. The following shows a sample output:

```
SanJose1#show dialer
BRI0/0 - dialer type = ISDN

Dial String      Successes   Failures    Last DNIS   Last status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0/0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

BRI0/0:2 - dialer type = ISDN
```



```
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

4. What is the idle timer set to for both BRI0/0:1 and BRI0/0:2?

____

____

Step 4

Now configure the Capetown router. The steps to accomplish this are basically the same as Steps 2 through 3. Therefore, complete the following:

```
Capetown(config)#isdn switch-type basic-ni
Capetown(config)#username SanJose1 password cisco
Capetown(config)#enable password cisco
Capetown(config)#line vty 0 4
Capetown(config-line)#password cisco
Capetown(config-line)#login
Capetown(config-line)#exit
Capetown(config)#interface bri0/0
Capetown(config-if)#ip address 192.168.16.3 255.255.255.0
Capetown(config-if)#encapsulation ppp
Capetown(config-if)#ppp authentication chap
Capetown(config-if)#dialer-group 1
Capetown(config-if)#isdn spid1 51055520000001 5552000
Capetown(config-if)#isdn spid2 51055520010001 5552001
Capetown(config-if)#dialer idle-timeout 60
Capetown(config-if)#dialer map ip 192.168.16.1 name SanJose1 5551000
Capetown(config-if)#no shutdown
```

Capetown is a stub network. All traffic destined for other networks other than its own should be forwarded to SanJose1. For this reason, enter a default static route on Capetown pointing to SanJose1 as follows:

```
Capetown(config)#ip route 0.0.0.0 0.0.0.0 192.168.16.1
```

Finally, to test and confirm connectivity between both sites, configure a more permissive dialer-list as follows:

```
Capetown(config)#dialer-list 1 protocol ip permit
```

Once connectivity has been confirmed between the two routers, a more restrictive dialer-list will be configured on Capetown.

Step 5

Test the ISDN connection. Before bringing up the ISDN link, enable debugging on both routers. This will allow for troubleshooting more efficiently in the event problems are encountered. Issue the following command to view dialer information on both routers:

```
SanJose1#debug dialer
```

ISDN may need to be debugged with the following command:

```
SanJose1#debug isdn events
```


Finally, because PPP with CHAP authentication is being used, also debug PPP as follows:

```
SanJose1#debug ppp authentication
SanJose1#debug ppp negotiation
```

Now, ping Host A from Host B. There will be a number of debug outputs. These will include a dialer debug on Capetown that should report the following:

```
00:56:00: BRI0/0 DDR: Dialing cause ip (s=192.168.216.2, d=192.168.0.2)
00:56:00: BRI0/0 DDR: Attempting to dial 5551000
```

Also, Capetown should report that channel B1 is now up, as the following shows:

```
00:56:01: %LINEPROTO-5-UPDOWN:Line protocol on Interface BRI0/0:1,changed state
to up
00:56:06: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5551000
SanJose1
```

Troubleshoot this connection as necessary. Use the debug output for clues. The **clear interface bri0/0** command may need to be used several times on both routers to reset the interfaces.

Note: To manually disconnect an ISDN call on BRI0/0, use the following command:

```
SanJose1#isdn disconnect interface bri0/0 [all, b1, b2]
```

Continue testing the ISDN connection, ping Host A from Host B and Host B from Host A.

The **show isdn history** command can also be issued to view all active and prior ISDN connections. The **show isdn active** command will output information about the current active connection. The following are sample outputs of both commands:

```
SanJose1#show isdn history
--------------------------------------------------------------------------------
                                ISDN CALL HISTORY
--------------------------------------------------------------------------------
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
--------------------------------------------------------------------------------
Call    Calling      Called       Remote  Seconds Seconds Seconds Charges
Type    Number       Number       Name    Used    Left    Idle
Units/Currency
--------------------------------------------------------------------------------
In                                           Failed
Out +ilable----     5551000     Capetown       60
Out +ilable----     5551000     Capetown       40      19      40
--------------------------------------------------------------------------------


Capetown#show isdn active
--------------------------------------------------------------------------------
                                ISDN ACTIVE CALLS
--------------------------------------------------------------------------------
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
--------------------------------------------------------------------------------
Call    Calling      Called       Remote  Seconds Seconds Seconds Charges
Type    Number       Number       Name    Used    Left    Idle
Units/Currency
--------------------------------------------------------------------------------
```



```
Out                 5551000     SanJose1       18       44       15       0
---------------------------------------------------------------------------------
```

Step 6

Now that there is a working ISDN connection, configure a more restrictive **dialer-list** on the Capetown remote router to keep ISDN charges to a minimum.

Create an access list to specifically permit web, DNS, FTP, Telnet, and mail traffic. For this to be done, reconfigure **dialer list 1** on Capetown, the remote router. The central site router, SanJose1, will continue to be allowed to establish DDR connections for any IP traffic.

Use the following to create an access list on Capetown that will permit the mission critical services:

```
Capetown(config)#access-list 101 permit tcp any any eq www
Capetown(config)#access-list 101 permit udp any any eq domain
Capetown(config)#access-list 101 permit tcp any any eq ftp
Capetown(config)#access-list 101 permit tcp any any eq telnet
Capetown(config)#access-list 101 permit tcp any any eq pop3
Capetown(config)#access-list 101 permit tcp any any eq smtp
```

Note: Transport layer keywords were specified instead of port numbers. Layer 4 keyword services are simpler to interpret when configuring extended access-lists. Use the “**?**” option after the **eq** parameter to receive a list of keywords and their associated port numbers.

Now enter a new dialer-list command that references this access list. The following shows a new dialer-list command automatically replacing the old one:

```
Capetown(config)#dialer-list 1 protocol ip list 101
```

Once the new dialer list has been configured, ping Host A from Host B.

5. The ping should fail, why?

____

____

From Host B initiate a Telnet session to SanJose1.

6. The Telnet request should bring up the ISDN connection, why?

____

____

With the connection still up, ping Host A from Host B once again.

7. Instead of failing as before, this ping should work. Why?

____

____

A ping to Host B from Host A should also be possible.

While connected, issue the **show dialer** command on both SanJose1 and Capetown.

8. According to the output of this command, what was the time until disconnect for SanJose1?

____

